PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-072450
(43)Date of publication of application : 19.03.1996

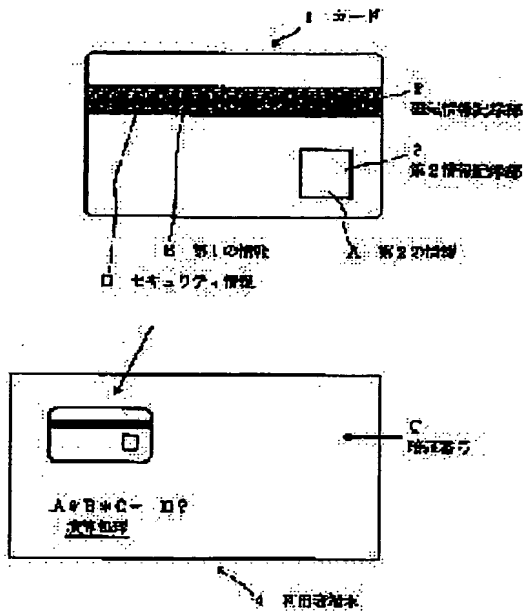
(51)Int.Cl. B42D 15/10
G03H 1/18
G06F 19/00
G06K 17/00
G06K 19/10
G06K 19/06
G09C 1/00

(21)Application number : 06-230185
(22)Date of filing : 01.09.1994

(71)Applicant : DAINIPPON PRINTING CO LTD
(72)Inventor : EMOTO SATOSHI

(54) CARD, CARD SECURITY SYSTEM AND CARD SECURITY METHOD

(57)Abstract:
PURPOSE: To provide a card high in safety preventing the unjust tapping of a secret number from the data communication circuit between a user terminal and a host computer and not forged to be abused.
CONSTITUTION: In a card 1, the first data B being the card inherent data such as the account number and security data D are stored in a magnetic data memory part 2 and second data A is provided to a second data memory part 3 due to a separate recording system such as a hologram storing security data D and impossible to view and read and possible to mechanically read are provided. The user terminal 4 judges whether a user is a correct card prossesor on the basis of whether three kinds of data of the inputted secret number C, first data and second data coincide with security data of special algorithm processing result data.



LEGAL STATUS

[Date of request for examination] 29.08.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3475304
[Date of registration] 26.09.2003
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁(JP)　(12)特許公報（Ｂ２）　(11)特許番号

特許第３４７５３０４号
（Ｐ３４７５３０４）

(45)発行日　平成15年12月8日(2003.12.8)　(24)登録日　平成15年9月26日(2003.9.26)

(51)Int.Cl.⁷	識別記号	FI		
Ｂ４２Ｄ	15/10	５０１	Ｂ４２Ｄ	15/10	５０１　Ａ
					５０１　Ｇ
					５０１　Ｐ
Ｇ０３Ｈ	1/18		Ｇ０３Ｈ	1/18	
Ｇ０６Ｋ	17/00		Ｇ０６Ｋ	17/00	Ｓ

請求項の数４　（全５頁）　最終頁に続く

(21)出願番号　特願平6-230185

(22)出願日　平成6年9月1日(1994.9.1)

(65)公開番号　特開平8-72450

(43)公開日　平成8年3月19日(1996.3.19)

審査請求日　平成13年8月29日(2001.8.29)

(73)特許権者　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目1番1号

(72)発明者　恵本　聡
東京都新宿区市谷加賀町一丁目1番1号　大日本印刷株式会社内

(74)代理人　100111659
弁理士　金山　聡

審査官　平井　聡子

最終頁に続く

(54)【発明の名称】カード、カードセキュリティシステム及びカードセキュリティ方法

1

(57)【特許請求の範囲】

【請求項１】　磁気情報記録部にカード固有の第１の情報と、セキュリティ情報とを有し、第２情報記録部に磁気以外の記録方式であって記録された情報の内容が機械読み取り可能で且つ目視判別出来ない第２の情報を有するカードであって、

上記第１の情報と上記第２の情報と、正当なカード所有者が記憶する暗証番号との３種類の情報を一定のアルゴリズムで演算処理して得られる結果情報が、前記セキュリティ情報であることを特徴とするカード。

【請求項２】　上記第２情報記録部が、第２の情報をホログラム再生像として有するホログラムからなることを特徴とする請求項１記載のカード。

【請求項３】　請求項１又は２記載のカードと、カード利用者が利用する利用端末と、からなり、

2

利用端末は、前記カードの磁気情報記録部に記録された第１の情報と、磁気以外の記録方式による第２情報記録部に記録された第２の情報と、磁気情報記録部に記録されたセキュリティ情報とを読み取り、読み取った第１の情報及び第２の情報と、カード利用者によって入力された暗証番号との３種類の情報を、一定のアルゴリズムで演算処理して得られる結果情報を、前記セキュリティ情報と照合して一致した場合に、

カード利用者が正当なカード所有者であると判定するカードセキュリティシステム。

【請求項４】　カードの磁気情報記録部に記録されたカード固有の第１の情報と、セキュリティ情報と、前記カードの第２情報記録部に記録された磁気以外の記録方式であって記録された情報の内容が機械読み取り可能で且つ目視判別出来ない第２の情報と、カード利用者から利

用者端末に入力される暗証番号との４種類の情報を利用して、

入力された暗証番号と、前記第１の情報と、前記第２の情報との３つの情報を、一定のアルゴリズムで演算処理して得られる結果情報が、前記セキュリティ情報と一致した場合に、カード利用者が正当なカード所有者であると判定するカードセキュリティ方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、カード類を利用して、ＣＤやＡＴＭ等の利用者端末を利用する際に、正当なカード所有者を識別するに適したカード、カードセキュリティシステム及びその方法に関し、特に、利用者が入力する暗証番号を通信回線から不正に取得してカードを偽造し悪用されることのない、安全なカード、セキュリティシステム及びその方法に関する。

【０００２】

【従来の技術】従来、銀行等のキャッシュカード取引の場合、利用者は、ＣＤやＡＴＭ等の利用者端末にカードを入れ、さらに利用者が記憶する暗証番号を入力することで、正当なカードの所有者としての認証を得ている。一方、利用者端末側では、入力された利用者の暗証番号をカードに記録されている口座番号等のカード固有情報と共に、ホストコンピュータに公衆回線又は専用回線を用いて送信し、ホストコンピュータは、送信された口座番号と暗証番号の組が正しいか否かを、記録保存してある口座番号と暗証番号とから判断し、正しければ、利用者端末側に、現在利用しようとする利用者が正当なカード所有者である旨の返信を行い、これに従い利用者端末は所定のカード取引処理を行っている。

【０００３】

【発明が解決しようとする課題】しかしながら、上記の様な利用者端末とホストコンピュータとを回線で結んで、利用者が正当なカード所有者であるか否かの認証を行うシステムでは、カード固有情報と共に利用者が記憶している暗証番号も回線を経由してデータ通信が行われている。このため、盗聴器を利用して、ハッカー等が回線からデータ通信される顧客取引データに係る信号を盗聴し解析することで、口座番号等と暗証番号とを不正に取得する可能性もあり得、これに基づいてカードを偽造すれば、何時盗聴したかも判らずに、元のカードを入手することなく、カード利用者に偽造されたと気付かれずに、比較的簡単に偽造カードが作られ、悪用される可能性があった。このため、通信回線を地下埋設する等して、盗聴器を仕掛けられにくくしたり、万が一、盗聴されても安全な様に、送受信するデータを各種方法で暗号化する等の対応も実施されて来たが、盗聴側で暗号のアルゴリズムが一旦解析されてしまえば安全性の確保は出来なくなり、完全なものではなかった。このようなことは、ホストコンピュータと利用者とにしか分からない暗

証番号の情報が通信回線を経由してデータ通信されることに起因する。かといって、暗証番号を回線で送信せずにカード自身に記録しておくことも考えられるが、従来の磁気記録方式では、カードさえ手に入れれば、磁気カードリーダライタによって、容易に暗証番号が盗用されてしまい実用的とはいえなかった。

【０００４】そこで、本発明の目的は、以上の如き従来の欠点を解決した、データ盗聴が完全に不可能であり、これに基づくカード偽造の途を断絶し、正当なカード所有者の判定が可能となる、安全性の高い、カード、カードセキュリティシステム及びカードセキュリティ方法を提供することである。

【０００５】

【課題を解決するための手段】上記目的を達成するために、本発明のカードは、磁気情報記録部にカード固有の第１の情報と、セキュリティ情報とを有し、第２情報記録部に磁気以外の記録方式であって記録された情報の内容が機械読み取り可能で且つ目視判別出来ない第２の情報を有するカードであって、上記第１の情報と上記第２の情報と、正当なカード所有者が記憶する暗証番号との３種類の情報を一定のアルゴリズムで演算処理して得られる結果情報が、前記セキュリティ情報である構成とする。また、上記カードにおいて、上記第２情報記録部が、機械読み取り可能な情報をホログラム再生像として有するホログラムからなる構成とするものである。

【０００６】また、本発明のカードセキュリティシステムは、上記カードと、カード利用者が利用する利用端末と、からなり、利用端末は、前記カードの磁気情報記録部に記録された第１の情報と、磁気以外の記録方式による第２情報記録部に記録された第２の情報と、磁気情報記録部に記録されたセキュリティ情報とを読み取り、読み取った第１の情報及び第２の情報と、カード利用者によって入力された暗証番号との３種類の情報を、一定のアルゴリズムで演算処理して得られる結果情報を、前記セキュリティ情報と照合して一致した場合に、カード利用者が正当なカード所有者であると判定するシステムである。

【０００７】また、本発明のカードセキュリティ方法は、カードの磁気情報記録部に記録されたカード固有の第１の情報と、セキュリティ情報と、前記カードの第２情報記録部に記録された磁気以外の記録方式であって記録された情報の内容が機械読み取り可能で且つ目視判別出来ない第２の情報と、カード利用者から利用者端末に入力される暗証番号との４種類の情報を利用して、入力された暗証番号と、前記第１の情報と、前記第２の情報との３つの情報を、一定のアルゴリズムで演算処理して得られる結果情報が、前記セキュリティ情報と一致した場合に、カード利用者が正当なカード所有者であると判定する方法である。

【０００８】

【作用】本発明のカード、カードセキュリティシステム及びカードセキュリティ方法によれば、カード利用者が正当なカード所有者であることを判定するキー情報となる暗証番号は、電話回線等を経由して伝送されることがなく、利用者端末内で判定ができる。しかも、暗証番号の正当性を判定する為に利用される情報が、磁気記録方式以外による第２情報記録部に記録され、係る情報が不可視であり、そこに記録される第２情報は容易に取得できない。そして、暗証番号の正当性は、利用者端末に入力された暗証番号と、前記第１の情報とこの第２情報との３種類の情報を一定のアルゴリズムで演算処理した結果得られる結果情報が、磁気情報記録部に記録されたセキュリティ情報と一致するか否かによって、判定される。磁気情報記録部に記録されたセキュリティ情報は、どちらかといえば、容易に取得できる情報であるが、もしもセキュリティ情報を不正に取得されても、第２の情報の取得が困難である上に、暗証番号、第１の情報、第２の情報及びセキュリティ情報との関係が、或る一定のアルゴリズムに基づいているので、第１の情報とセキュリティ情報とから暗証番号を導き出すことは困難であり、第２の情報がたとえ不正に取得されても、アルゴリズムの演算処理を逆演算して、暗証番号を導き出すことは、困難である。

【０００９】

【実施例】以下、本発明のカード、カードセキュリティシステム及びカードセキュリティ方法について詳述する。

【００１０】図１は、本発明のカード、カードセキュリティシステム及びカードセキュリティ方法を説明する説明図である。カード１には、通常の磁気記録方式による磁気情報記録部２と、磁気方式以外の方式であって、記録された情報の内容が不可視の第２情報記録部３とを有する。そして、磁気情報記録部２には、例えば、キャッシュカードであれば、カード利用者の銀行番号、支店番号、口座番号等からなるカード固有の第１の情報Ｂが記録されている。また、磁気情報記録部２には、後述する関係を有するセキュリティ情報Ｄも記録されている。また、第２情報記録部３には、一定のアルゴリズムの演算で使用する、コード情報や画像情報からなる第２の情報Ａが記録されている。

【００１１】そして、上記した第２の情報Ａと、第１の情報Ｂと、セキュリティ情報Ｄと、正当なカード所有者が記憶する暗証番号Ｃとは、或る特定な関係を有する。すちわち、第２の情報Ａと、第１の情報Ｂと、暗証番号Ｃとの３種類の情報を或る一定のアルゴリズム、例えば、暗号化処理、による演算処理を行った結果情報が、磁気情報記録部に記録されているセキュリティ情報Ｄと一致するような、情報の関係を有するカードとなっている。

【００１２】これら四者の情報の関係を数式で表せば、

Ａ＊Ｂ＊Ｃ＝Ｄ

（＊は或る一定のアルゴリズムによる演算処理を表す）

となる。なお、「Ａ＊Ｂ＊Ｃ」は、Ａ＊Ｂの演算処理を行って得られた結果情報と、Ｃとを更に一定のアルゴリズムによって演算処理する意味も有するが、Ａ、Ｂ、Ｃに対する演算の順序は、任意であり、特に制限されない。また、Ａ＊ＢとＢ＊ＣとＡ＊Ｃとして、三者をそれぞれ演算することもあり得る。また、演算記号「＊」の前と後にくる情報の前後関係が逆になると演算結果が異なる演算もあり得る。要するに、ＡとＢとＣとを用いて演算を行う意味を表す。

【００１３】セキュリティ情報Ｄは、第２の情報Ａと、第１の情報Ｂと、暗証番号Ｃとの３種類の情報を或る一定のアルゴリズムによる演算処理を行った結果情報に相当するが、例えば、前記３種類の情報が、全て数値であり、演算結果も数値であるとすれば、セキュリティ情報は、演算結果の数値の各桁から導き出すチェックディジット情報等でも良い。また、セキュリティ情報は、前記３種類の情報の演算処理結果の全ての情報を含むものであることは、必ずしも必要ではない。但し、このような場合でも、演算結果の情報の一部を抽出するという演算処理を施しいていると解することができる。

【００１４】もしも、不正利用者によって、第２の情報Ａが容易に取得され、暗証番号Ｃが分からなくても、複数枚の不正入手したカードの第２の情報Ａと、第１の情報Ｂと、セキュリティ情報Ｄとから、逆演算をしたり、パーソナルコンピュータを利用して試行錯誤によりランダムに発生した暗証番号によって一定のアルゴリズムが解析されることができるような簡単なアルゴリズムであるならば、セキュリティは低下してしまう。従って、上記する演算処理は、通常、暗号化処理等として使用されている、特殊な演算処理を使用することが好ましい。

【００１５】また、第２の情報が記録される第２情報記録部は、目視判別できず、磁気記録部と同様な方式での読み取りを困難にするという点で、磁気記録方式以外の方式によるものとする。このような点から、第２情報記録部としては、例えば、バーコードを目視不可能に隠蔽したものや、機械読み取り可能なホログラム、紫外線や赤外線等の可視光以外の光を照射した時のみ機械読み取りが可能となる等の目視不可能なインキで形成したコードパターン等、各種機械読み取りが可能な形態のものが使用できる。

【００１６】第２情報記録部としては、上記のなかでも、機械読み取り可能な画像情報を再生像として有するホログラムが好ましい。このようなホログラムとすれば、係る画像情報から、例えば、コード情報等の情報を読み取るには、特殊な読み取り装置が必要となり、容易に装置を入手することができないため、読み取りは困難となるからである。

【００１７】さらに、第２情報記録部に記録される第２

情報を、所定のアルゴリズムで暗号化して記録したり、装置の読み取り処理過程でデータスクランブル処理をしたりすれば、たとえ、読み取り装置が入手できたとしても、よりセキュリティを高いものとすることができる。

【００１８】以上のようにうして、正当なカード所有者が記憶している暗証番号が、利用者端末に入力されれば、利用者端末は、ホストコンピュータの助けを借りること無く、独自にカード利用者の正当性を判断することができる。そして、カード利用者が正当なカード所有者であると、利用者端末が判断すれば、利用者端末側で、或いはホストコンピュータと所定のデータ交信を行った後、ホストコンピュータ側で、利用者に対してカード利用の認証を行い、利用者端末は、カード利用者が要求する処理を実行することとなる。なお、カード利用者に対する最終的な取引承認は、利用者端末側独自でもできるが、ホストコンピュータ側で最終的な取引承認を行う場合には、係るカード利用者が、そのカードの正当な所有者である以外に、別の選択基準によるカード利用権保持者であることに基づいて、取引承認を行うことができる。これは、例えば、カードを紛失して、当該カードについて取引停止処理をホストコンピュータ側で行った場合等に有効となる。

【００１９】

【発明の効果】以上詳述した如く本発明のカード、カードセキュリティシステム、カードセキュリティ方法によれば、極めて安全性の高い、正当なカード所有者の判定を可能とするに適したカードとなる。カードとしては、不正にカードを入手したとしても、暗証番号の情報は記録されておらず、暗証番号まで知り得ることは不可能である。また、万が一、暗証番号を不正に入手されたとしても、当該磁気記録方式以外の記録部を有するカードも入手されない限り、カードの不正利用は不可能である。また、カード固有の情報である第１の情報とセキュリティ情報とを不正に入手したとしても、第２の情報の入手は困難であり、たとえ、第２の情報も入手したとしても、これら３種類の情報から暗証番号を入手するには一定のアルゴリズムを取得しない限り不可能であり、極めて難しい。また、第２情報記録部に、機械読み取り可能なホログラムを用いれば、第２情報記録部に記録されている第２情報の不正入手は、ホログラムの再生像から情報を読み取る専用の装置を入手しなければ、不可能であり、第２情報の入手は極めて困難となる。

【００２０】カードセキュリティシステムとしては、それを構成するカードとしては上記する効果を有する。また、利用者端末側としては、カード利用者がカードの正当な所有者であるという正当性の判定のキー情報となる暗証番号を、通信回線によってホストコンピュータにデータ通信せずにて判定するので、通信回線の盗聴による情報の不正入手が完全に不可能となり、盗聴データに基づく不正カードの偽造は完全に防止でき、盗聴に対して極めてセキュリティの高いシステムとなる。また、第２情報記録部に機械読み取り可能なホログラムを利用すれば、第２情報記録に記録された情報の読み取りは、特殊な装置を入手しなければ行えず、システムとしても、セキュリティの高いものとなる。

【００２１】カードセキュリティ方法としては、上記するようにデータ通信過程による盗聴が完全に防止できる他に、４種類の情報を暗号化処理等の或る一定のアルゴリズムによる演算処理で関係を判断し、且つこれらの情報のうち、暗証番号はシステム以外の正当なカード利用者の記憶情報であり、第２の情報は磁気記録方式以外の容易に読み取ることが出来ない情報とし、これらを場所的、記録形式的に分散しているために、カード利用者が正当なカード所有者であるか否かの判定は極めてセキュリティが高いこととなる。

【００２２】さらに、本発明のカード、カードセキュリティシステム、カードセキュリティ方法によれば、上述のデータ通信の盗聴対策等に効果的であるばかりでなく、従来の磁気記録方式のカードで可能性があった、ＣＤやＡＴＭのコーナーで取引後に利用者がゴミ箱等に廃棄したレシート（利用明細票）から利用者の口座番号を不正入手し、さらに取引時に暗証番号を盗み見て、偽造カードで現金を引き出すといった悪用を、確実に防止できる。

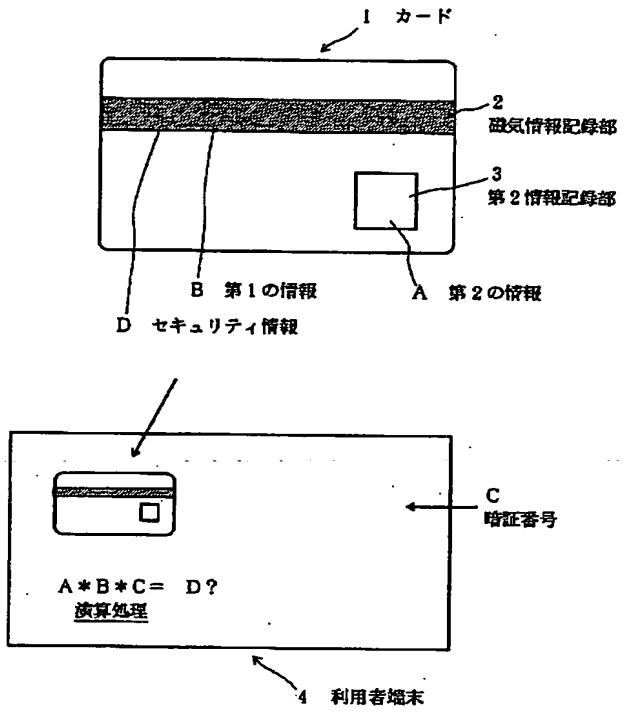
【図面の簡単な説明】

【図１】本発明のカード、カードセキュリティシステム及びカードセキュリティ方法を説明する説明図。

【符号の説明】

１　カード
２　磁気情報記録部
３　磁気以外の記録方式による第２情報記録部
Ａ　第２情報
Ｂ　カード固有情報
Ｃ　暗証番号（利用者記憶情報）
Ｄ　セキュリティ情報

【図１】



フロントページの続き

(51) Int. Cl. ⁷	識別記号	FI	
Ｇ０６Ｋ　19/06		Ｇ０９Ｃ　1/00	
19/10		Ｇ０６Ｋ　19/00	Ｒ
Ｇ０９Ｃ　1/00			Ｄ

(56) 参考文献
- 特開　平６－143746（ＪＰ，Ａ）
- 特開　昭62－212974（ＪＰ，Ａ）
- 特開　昭62－35892（ＪＰ，Ａ）
- 特開　昭63－159094（ＪＰ，Ａ）
- 特開　平６－115287（ＪＰ，Ａ）
- 特開　平６－135187（ＪＰ，Ａ）
- 特開　平５－262078（ＪＰ，Ａ）

(58) 調査した分野 (Int. Cl. ⁷，ＤＢ名)
- B42D　5/00 - 15/10
- G06K　17/00
- G06K　19/00